# EXHIBIT E

# FILED UNDER SEAL

MJ: Now, you do understand if you do read the statement and you tell me something that's not true, that the statement can be used against you later for charges of perjury or making false statements?

ACC: Yes, Your Honor.

MJ: Your counsel has asked for a brief recess. What we're going to do is we'll take that brief recess, we'll come back, you can read your statement, and then we'll go over -- I'll be oriented to the facts, we'll go over each of the specifications that you're pleading guilty to at that time.

How long would you like for a recess?

CDC[MR.COOMBS]: Just 10 minutes, Your Honor.

MJ: All right.

TC[MAJ FEIN]: Ma'am, if we can just make it 15 because of the number of spectators?

MJ: Why don't we just do that? We'll just reconvene here at 11 o'clock. Court is in recess.

**[The Article 39(a) session recess at 1050, 28 February 2013.]**

**[The Article 39(a) session was called to order at 1109, 28 February 2013.]**

MJ: This Article 39(a) session is called to order. Let the record reflect all parties present when the court last recessed are again present in court. PFC Manning, you may read your statement.

ACC: Yes, Your Honor. I wrote this statement in confinement, so I'll start now. The following facts are provided in support of the providence inquiry for my court-martial, United States v. PFC Bradley E. Manning.

Personal facts: I'm a 25 year-old Private First Class in the United States Army currently assigned to Headquarters and Headquarters Company (HHC), U.S. Army Garrison (USAG), Joint Base Myer-Henderson Hall, Fort Myer, Virginia. Prior to this assignment, I was assigned to HHC, 2nd Brigade Combat Team, 10th Mountain Division at Fort Drum, New York. My Primary Military Occupational Specialty or PMOS is 35F, Intelligence Analyst. I entered active duty status on 2 October 2007. I enlisted with the hope of obtaining both real-world experience and earning benefits under the G.I. Bill for college opportunities.

Facts regarding my position as an intelligence analyst: In order to enlist in the Army, I took the Standard Armed Services Aptitude Battery or ASVAB. My score on this battery was high enough for me to qualify for any enlisted MOS position. My recruiter informed me that I should select an MOS that complemented my interests outside the military. In response, I told him that I was interested in geopolitical matters and information technology. He suggested that I consider becoming an intelligence analyst.

After researching the intelligence analyst position, I agreed that this would be a good fit for me. In particular, I enjoyed the fact that an analyst would use information derived from a variety of sources to create work products that informed the command of its available choices for determining the best course of action or COAs. Although the MOS required a working knowledge of computers, it primarily required me to consider how raw information could be combined with other available intelligence sources in order to create products that assist in the command and its situational awareness or SA.

I assessed that my natural interest in geopolitical affairs and my computer skills would make me an excellent intelligence analyst. After enlisting, I reported to the Fort Meade Military Entrance Processing Station on 1 October 2007. I then traveled to and reported at Fort Leonard Wood, Missouri on 2 October 2007 to begin Basic Combat Training or BCT.

Once at Fort Leonard Wood, I quickly realized that I was neither physically nor mentally prepared for the requirements of basic training. My BCT experience lasted 6 months instead of the normal 10 weeks. Due to medical issues, I was placed on a hold status. A physical examination indicated that I sustained injuries to my right shoulder and left foot. Due to those injuries, I was unable to continue Basic. During medical hold, I was informed that I

may be out processed from the Army, however, I resisted being chaptered out because I felt I could overcome my medical issues and continue to serve.

On 20 January 2008, I returned to Basic Combat Training. This time, I was better prepared and I completed training on 2 April 2008. I then reported for the MOS-specific Advanced Individual Training or AIT on 7 April 2008.

AIT was an enjoyable experience for me. Unlike Basic Training where I felt different from the other Soldiers, I fit in and did well. I preferred the mental challenges of reviewing a large amount of information from various sources and trying to create useful or actionable products. I especially enjoyed the practice of analysis through the use of computer applications and methods I was familiar with.

I graduated from AIT on 16 August 2008 and reported to my first duty station, Fort Drum, New York on 28 August 2008. As an analyst, Significant Activities or SIGACTs were a frequent source of information for me to use in creating work products.

I started working extensively with SIGACTS early after my arrival at Fort Drum. My computer background allowed me to use the tools organic to the Distributed Common Ground System-Army or DCGS-A computers to create polished work products for the 2nd Brigade Combat Team chain of command.

The noncommissioned officer in charge, or NCOIC, of the S-2 section, then Master Sergeant David P. Adkins, recognized my skills and potential and tasked me to work on a tool abandoned by a previously assigned analyst, the incident tracker. The incident tracker was viewed as a backup to the Combined Information Data Network Exchange or CIDNE and as a unit historical reference tool.

In the months preceding my upcoming deployment, I worked on creating a new version of the incident tracker and used SIGACTS to populate it. The SIGACTs I used were from Afghanistan because, at the time, our unit was scheduled to deploy to the Logar and Wardak Provinces of Afghanistan. Later, our unit was reassigned to deploy to Eastern Baghdad, Iraq. At that point, I removed the Afghanistan SIGACTs switch to Iraq SIGACTs.

As an analyst, I viewed the SIGACTs as historical data. I believe this view is shared by other all-source analysts as well. SIGACTs give a first-look impression of a specific or isolated event. This event can be an Improvised Explosive Device attack, or IED; Small Arms Fire engagement, or SAF; engagement with a hostile force or any other event a specific unit documented and reported in real time. In my perspective, the information contained within a single SIGACT or group of SIGACTs is not very sensitive. The events encapsulated within most SIGACTs involve either enemy engagements or casualties. Most of this information is publicly reported by the

public affairs office or PAO, embedded media pools, or host nation (HN) media.

As I started working with SIGACTs, I felt they were similar to a daily journal or log that a person may keep. They capture what happens on a particular date and time. They are created immediately after the events and are potentially updated over a period of hours until a final version is published on the CIDNE -- on the Combined Information Data Network Exchange. Each unit has its own Standard Operating Procedure or SOP for reporting and recording SIGACTs. The SOP may differ between reporting in a particular deployment and reporting in garrison. In garrison, a SIGACT normally involves personnel issues such as driving under the influence or DUI incidents or an automobile involving the death or serious injury of a Soldier. The report starts at the company level and goes up to the battalion, brigade, and even up to the division level.

In a deployed environment, a unit may observe or participate in an event and a platoon leader or platoon sergeant may report the event to a SIGACT -- as a SIGACT to the company headquarters through the Radio Transmission Operator or RTO. The commander or RTO will then forward the report to the battalion battle captain or battle noncommissioned officer or NCO. Once the battalion battle captain or battle NCO receives the report, they will either, one, notify the battalion operations officer or S-3, two, conduct an

action such as launching the quick reaction force or, three, record the event and report -- and further report it up the chain of command to the brigade. The recording of each event is done by radio or over the Secret Internet Protocol Router Network or SIPRNET, normally by an assigned Soldier, usually junior-enlisted, E4 and below. Once the SIGACT is reported, the SIGACT is further sent up the chain of command. At each level, additional information can either be added or corrected as needed. Normally, within 24 to 48 hours, the updating or recording of a particular SIGACT is complete. Eventually, all reports and SIGACTs go through the chain of command from brigade to division and division to corps. At corps level, the SIGACT is finalized and published.

The CIDNE system contains a database that is used by thousands of Department of Defense (DoD) personnel, including Soldiers, civilians, and contractor support. It was the United States Central Command or CENTCOM reporting tool for operational reporting in Iraq and Afghanistan. Two separate but similar databases were maintained for each theater: CIDNE-I for Iraq and CIDNE-A for Afghanistan. Each database encompasses over 100 types of reports and other historical information for access. They contain millions of vetted and finalized records including operational intelligence reporting. CIDNE was created to collect and analyze battle space data to provide daily operational and Intelligence

Community (IC) reporting relevant to a commander's daily decision-making process. The CIDNE-I and CIDNE-A databases contain reporting and analysis fields from multiple disciplines including Human Intelligence or HUMINT Reports, Psychological Operations or PYSOP reports, engagement reports, Counter-Improvised Explosion Device or CIED reports, SIGACT reports, targeting reports, social and cultural reports, civil affairs reports, and human terrain reporting.

As an intelligence analyst, I had unlimited access to the CIDNE-I and CIDNE-A databases and the information contained within them. Although each table within the database is important, I primarily dealt with HUMINT reports, SIGACT reports, and Counter-IED reports because these reports were used to create the work product I was required to publish as any analyst.

When working on an assignment, I looked anywhere and everywhere for information. As an all-source analyst, this was something that was expected. The DCGS-A systems had databases built in and I utilized them on any daily basis. This includes the search tools available on DCGS-A systems on SIPRNET such as Query Tree, and the DOD and Intelink search engines. Primarily, I utilized the CIDNE database using the historical and HUMINT reporting to conduct my analysis and provide back-up for my end work product. I did statistical analysis on historical data including SIGACTs to backup analyses that were based on HUMINT reporting and produced charts,

graphs, and tables. I also created maps and charts to conduct predictive analysis based on statistical trends. The SIGACT reporting provided a reference point for what occurred and provided myself and other analysts with the information to conclude possible outcomes.

Although SIGACT reporting is sensitive at the time of their creation, their sensitivity normally dissipates within 48 to 72 hours as the information is either publicly released, the unit involved is no longer in the area and not in danger -- or the unit involved is no longer in the area and not in danger. It is my understanding that the SIGACT reports remain classified only because they are maintained within CIDNE because it is only accessible on SIPRNET. Everything on CIDNE-I and CIDNE-A, to include SIGACT reporting, was treated as classified information.

Facts regarding the storage of SIGACT reports. As part of my training at Fort Drum, I was instructed to ensure that I create backups of my work product. The need to create backups was particularly acute given the relative instability and reliability of the computer systems we used in the field during the deployment. These computer systems included both organic and theater-provided equipment (TPE) DCGS-A machines.

The organic DCGS-A machines we brought with us into the field on our deployment were Dell M90 laptops and the TPE DCGS-A

machines were Alienware brand laptops. The M90 DCGS-A laptops were the preferred machine to use as they were slightly faster and had fewer problems with dust and temperature than the theater-provided Alienware laptops. I used several DCGS-A machines during the deployment due to various technical problems with laptops.

With these issues, several analysts lost information, but I never lost information due to the multiple backups I created. I attempted to backup as much relevant information as possible. I would save the information so that I, or another analyst, could quickly access it whenever a machine crashed, SIPRNET connectivity was down, or I forgot where the data was stored. When backing up information, I would do one or all of the following things based on my training:

Physical backup. I tried to keep physical backup copies of information on paper so that the information could be grabbed quickly. Also, it was easier to brief from hard copies of research in HUMINT reports.

Two, local drive backup. I tried to sort out information I deemed relevant and keep complete copies of the information on each of the computers I used in the Temporary Sensitive Compartmentalized -- Compartmented Information Facility, or T-SCIF, including my primary and secondary DCGS-A machines. This was stored under my user profile on the desktop.

Share drive -- or share drive backup. Each analyst had access to a T-drive -- what we called a "T-drive" -- shared across the SIPRNET. It allowed others to access information that was stored on it; S-6 operated the T-drive.

Compact Disc-Rewritable or CD-RW back up. For larger data sets, I saved the information onto a re-writable disc, labeled the discs, and stored them in the conference room of the T-SCIF. This redundancy permitted us the ability to not worry about information loss. If a system crashed, I could easily pull the information from a secondary computer, the T-drive, or one of the CD-RWs. If another analyst wanted to access my data but I was unavailable, she could find my published products directory on the T-drive or on the CD-RWs. I sorted all of my products and research by date, time, and group and updated the information on each of the storage methods to ensure that the latest information was available to them.

During the deployment, I had several of the DCGS-A machines crash on me. Whenever a computer crashed, I usually lost information but the redundancy method ensured my ability to quickly restore old backup data and add my current information to the machine when it was repaired or replaced.

I stored the backup CD-RWs of larger data sets in the conference room of the T-SCIF or next my workstations. I marked the CD-RWs based on the classification level and its content.

Unclassified CD-RWs were only labeled with content type and not marked with classification markings. Early on in the deployment, I only saved and stored the SIGACTs that were within or near our operational environment. Later, I thought it would be easier just to save all the SIGACTs on to a CD-RW. The process would not take very long to complete and so I downloaded the SIGACTs from CIDNE-I onto a -- onto a DCGS-on to a CD-RW. After finishing with CIDNE-I, I did the same with CIDNE-A. By retrieving the CIDNE-I and CIDNE-A SIGACTs, I was able to retrieve the information whenever I needed it and not rely upon the unreliable and slow SIPRNET connectivity needed to pull them. Instead, I could just find the CD-RW and open the pre-loaded spreadsheet. This process began in late December 2009 and continued through early January 2010. I could quickly export one month of the SIGACT data at a time and download in the background as I did other tasks. The process took approximately a week for each table.

After downloading the SIGACT tables, I periodically updated them by pulling only the most recent SIGACTs and simply copying them and pasting them into the database saved on the CD-RW. I never hid the fact that I had downloaded copies of both the SIGACT tables from CIDNE-I and CIDNE-A. They were stored on appropriately labeled and marked CD-RWs, stored in the open. I viewed the saved copies of the CIDNE-I and CIDNE-A SIGACT tables as being both for my use and the

use of anyone within S-2 section during the SIPRNET connectivity issues.

In addition to the SIGACT tables, I had a large repository of HUMINT reports and counter-IED reports downloaded from CIDNE-I. These contained reports that were relevant to the area in and around our operational environment in Eastern Baghdad and the Diyala Province of Iraq.

In order to compress the data to fit onto a CD-RW, I use a compression algorithm called "BZIP2." The program used to compress the data is called "WinRar." WinRar is an application that is free and can be easily downloaded from the internet via the Nonsecure Internet Relay Protocol Network, or NIPRNET. I downloaded WinRar on NIPRNET and transferred it to the DCGS-A machine user profile desktop using the CD-RW. I did not try to hide the fact that I was downloading WinRar onto my SIPRNET DCGS-A machine or computer. With the assistance of the BZIP2 compression algorithm, using the WinRar program, I was able to fit all the SIGACTs onto a single CD-RW and the relevant HUMINT and Counter-IED reports onto a separate CD-RW.

Facts regarding my knowledge of the WikiLeaks Organization or WLO: I first became vaguely aware of the WLO during my AIT at Fort Huachuca, Arizona, though I did not fully pay attention until WLO -- until the WLO released purported Short Messaging System or SMS messages from 11 September 2001 on 25 November 2009. At that time,

references to the release and the WLO website showed up in my daily Google News open-source search for information related to U.S. foreign policy. The stories were about how WLO published approximately 500,000 messages. I then reviewed the messages myself and realized that the posted messages were very likely real, given the sheer volume and detail of the content.

After this, I began conducting research on WLO. I conducted searches on both NIPRNET and SIPRNET on WLO beginning in late November 2009 and early 2000 -- early December 2009. At this time, I also began to routinely monitor the WLO website. In response to one of my searches in December 2009, I found the United States Army Counterintelligence Center or USACIC report on the WikiLeaks Organization. After reviewing the report, I believe that this report was one of the -- was possibly the one that my AIT instructor referenced in early 2008. I may or may not have saved the report on my DCGS-A workstation. I know I reviewed the document on other occasions throughout early 2010 and saved it on both my primary and secondary laptops.

After reviewing the report, I continued doing research on WLO, however, based upon my open-source collection, I discovered information that contradicted the 2008 USACIC report including information indicating that, similar to other press agencies, WLO seemed to be dedicated to exposing illegal activities and corruption.

WLO received numerous awards and recognition for its reporting activities.

Also, in reviewing the WLO website, I found information regarding U.S. military SOPs for Camp Delta at Guantánamo Bay, Cuba and information on the, then, outdated rules of engagement or ROE in Iraq for cross-border pursuits of former members of Saddam Hussein's al-Tikiriti's government.

After seeing the information available on the WLO website, I continued following it and collecting open-source information from it. During this time period, I followed several organizations and groups including wire press agencies such as the Associated Press and Reuters and private intelligence agencies including Strategic Forecasting or STRATFOR. This practice was something I was trained to do during AIT and was something that good analysts are expected to do.

During the searches of WLO, I found several pieces of information that I found useful in my work product -- in my work as an analyst, specifically, I recall WLO publishing documents related to weapons trafficking between two nations that affected my OE. I integrated this information into one or more of my work products. In addition to visiting the WLO website, I began following WLO using and Instant Relay Chat or IRC client called "XChat" sometime in early January 2010.

IRC is a protocol for real-time Internet communications by messaging and conferencing, colloquially referred to as chat rooms or chats. The IRC chat rooms are designed for group communication discussion forums. Each IRC chat room is called a channel. Similar to a television, you can tune in or follow it -- follow a channel so long as it is open and does not require an invite. Once joining a specific IRC conversation, other users in the conversation can see that you have joined the room. On the Internet, there are millions of different IRC channels across several services. Channel topics span a range of topics covering all kinds of interests and hobbies.

The primary reason for following WLO on IRC was curiosity, particularly in regards to how and why they obtained the SMS messages referenced above. I believed that -- I believed that collecting information on the WLO would assist me in this goal.

Initially, I simply observed the IRC conversations. I wanted to know how the organization was structured and how they obtained their data. The conversations I viewed were usually technical in nature, but sometimes switched to a lively debate on issues a particular individual may have felt strongly about.

Over a period of time, I became more involved in these discussions, especially when conversations turned to geopolitical events and information topics -- information technology topics such

as networking and encryption methods. Based on these observations, I would describe the WL organization as almost academic in nature.

In addition to the WLO conversations, I participated in numerous other IRC channels across at least three different networks. The other IRC channels I participated in normally dealt with technical topics including the LINUX and Berkley Security Distribution (BSD) operating systems or OSs, networking, encryption algorithms and techniques, and other more political topics such as politics and queer rights.

I normally engaged in multiple IRC conversations simultaneously; mostly publicly but often privately. The XChat client enabled me to manage these multiple conversations across different channels and servers. The screen for XChat was often busy, but experience enabled me to see when something was interesting. I would then select conversation and either observe or participate.

I really enjoyed the IRC conversations pertaining to and involving the WLO. However, at some point in late February or early March of 2010, the WLO IRC channel was no longer accessible. Instead, the regular participants of this channel switched to using a Jabber server.

Jabber is another Internet communication tool similar, but more sophisticated than IRC. The IRC and Jabber conversations

allowed me to feel connected to others, even when alone. They helped me pass the time and keep motivated throughout the deployment.

Facts regarding the unauthorized storage and disclosure of the SIGACTs: As indicated above, I created copies of the CIDNE-I and CIDNE-A SIGACT tables as part of the process of backing up information. At the time I did so, I did not intend to use this information for any purpose other than for backup. However, I later decided to release this information publicly. At that time, I believed and still believe that these tables are two of the most significant documents of our time.

On 8 January 2010, I collected the CD-RW I stored in the conference room of the T-SCIF and placed into the cargo pocket of my ACU or Army Combat Uniform. At the end of my shift, I took the CD-RW out of the T-SCIF and brought it to my Containerized Housing Unit or CHU. I copied the data onto my personal laptop. Later, at the beginning of my shift, I returned to -- I returned the CD-RW back to the conference room of the T-SCIF.

At the time I saved the SIGACTs to my laptop, I planned to take them -- I planned to take them with me on mid-tour leave and decide what to do with them. At some point prior to my mid-tour leave, I transferred the information from my computer to a Secure Digital memory card for my digital camera. The SD card for the

camera also worked on my computer and allowed me to store the SIGACT tables in a secure manner for transport.

I began mid-tour leave on 23 January 2010, flying from Atlanta, Georgia to Reagan National Airport in Virginia. I arrived at the home of my aunt, Debra M. Van Alstyne in Potomac, Maryland and quickly got in contact with my then boyfriend, Tyler R. Watkins.

Tyler, then a student at Brandeis University in Waltham, Massachusetts, and I made plans to -- for me to visit him in Boston, Massachusetts area. I was excited to see Tyler and planned on talking to Tyler about where our relationship was going and about my time in Iraq. However, when arrived in the Boston area, Tyler and I seem to become distant. He did not seem very excited about my return from Iraq. I tried talking to him about our relationship, but he refused to make any plans. I also tried raising the topic of releasing the CIDNE-I and CIDNE-A SIGACT tables to the public.

I asked Tyler hypothetical questions about what he would do if he had documents that he thought the public needed -- that the public needed access to. Tyler didn't really have a specific answer for me. He tried to answer the question and be supportive, but seemed confused by the question and its context. I then tried to be more specific, but he asked too many questions. Rather than try to explain my dilemma, I decided just to drop the conversation. After a few days in Waltham, I began feeling that I was overstaying my

welcome and I returned to Maryland. I spent the remainder of my time on leave in the Washington, D.C. area.

During this time, a blizzard bombarded the Mid-Atlantic and I spent a significant time period of time, essentially, stuck at my aunt's house in Maryland. I began to think about what I knew and the information I still had in my possession. For me, the SIGACTs represented the on-the-ground reality of both the conflicts -- both the conflicts in Iraq and Afghanistan. I felt we were risking so much for -- risking so much for people that seemed unwilling to cooperate with us leading to frustration and hatred on both sides.

I began to become depressed with the situation that we found ourselves increasingly mired in year after year. The SIGACTs documented this in great detail and provided context to what we were seeing on the ground. In attempting to conduct counterterrorism or CT and counterinsurgency (COIN) operations, we became obsessed with capturing/killing human targets on lists and on being suspicious and avoiding cooperation with our host nation partners and ignoring the second and third order effects of accomplishing short-term goals and missions.

I believe that if the general public, especially the American public, had access to the information contained within the CIDNE-I and CIDNE-A tables, this could spark a domestic debate on the role of the military and our foreign policy, in general, as well as

it related to Iraq and Afghanistan. I also believe the detailed analysis of the data over a long period of time by different sectors of society might cause society to reevaluate the need or even the desire to engage in counterterrorism and counterinsurgency operations that ignore the complex dynamics of the people living in the affected environment every day.

At my aunt's house, I debated what I should do with the SIGACTs; in particular, whether I should hold onto them or disclose them through a press agency. At this point, I decided it made sense to try and disclose the SIGACT tables to an American newspaper. I first called my local newspaper, the *Washington Post*, and spoke with a woman saying that she was a reporter. I asked her if the *Washington Post* would be interested in receiving information that would have enormous value to the American public. Although we spoke for about 5 minutes concerning the general nature of what I possessed, I do not believe she took me seriously. She informed me that the *Washington Post* would possibly be interested, but that such decisions were made only after seeing the information I was referring to and after consideration by the senior editors.

I then decided to contact the largest and most popular newspaper, the *New York Times*. I called the public editor number on the *New York Times* website. The phone rang and was answered by a machine. I went through the menu to the section for news tips and

was routed to an answering machine. I left a message stating that I had access to information about Iraq and Afghanistan that I believed was very important. However, despite leaving my Skype phone number and personal e-mail address, I never received a reply from the *New York Times*.

I also briefly considered dropping into the office for the political commentary blog, *Politico*, however, the weather conditions during my leave hampered my efforts to travel. After these failed efforts, I ultimately decided to submit the materials to the WLO. I was not sure if the WLO would actually publish the SIGACT tables or even if they would publish. I was concerned that they might -- I was also concerned that they might not be noticed by the American media. However, based upon what I read about the WLO through my research described above, they seemed to be the best medium for publishing this information to the world within my reach.

At my aunt's house, I joined in on an IRC conversation and stated I had information that needed to be shared with the world. I wrote that the information would help document the true costs of the wars in Iraq and Afghanistan. One of individuals in the IRC asked me to describe the information. However, before I could describe information, another individual pointed me to the link for the WLO website's online submission system. After ending my IRC connection,

I considered my options one more time. Ultimately, I felt that the right thing to do was to release the SIGACTs.

On 3 February 2010, I visited the WLO website on my computer and clicked on the "submit documents" link. Next, I found the "Submit Your Information Online" link and elected to submit the SIGACTs via the Onion Router or TOR (T-O-R) anonymizing network by a special link.

TOR is a system intended to provide anonymity online. Software routes Internet traffic through a network of servers and other TOR clients in order to conceal a user's location and identity. I was familiar with TOR and had it previously installed on my computer to anonymously monitor the social media websites and militia groups operating within central Iraq.

I follow the prompts and attached the compressed data files of CIDNE-I and CIDNE-A SIGACTs. I attached the text file I drafted while preparing to provide documents to the *Washington Post*. It provided rough guideline saying, "It's already been sanitized of any source-identifying information. You might need to sit on this information, perhaps 90 to 100 days, to figure out how to best release such a large amount of data and to protect the source. This is possibly one of the more significant documents of our time, removing the fog of war and revealing the true nature of 21st-century asymmetric warfare. Have a good day."

After sending this, I left the SD card in a camera case at my aunt's house in the event I needed it again in the future.

I returned from mid-tour leave on 11 February 2010. Although the information had not yet been publicly -- had not yet been published by the WLO, I felt a sense of relief by them having it. I felt I had accomplished something that allowed me to have a clear conscience based upon what I had seen and read about and knew were happening in both Iraq and Afghanistan every day.

Facts regarding the unauthorized storage and disclosure of 10 Reykjavík 13. I first became aware of the diplomatic cables during my training period in AIT. I later learned about the Department of State, or DoS, Net-Centric Diplomacy (NCD) portal from the 2/10 Brigade Combat Team S-2, Captain Steven Lim.

Captain Lim sent a section-wide e-mail to the other analysts and officers in late December 2009 containing the SIPRNET link to the portal along with the instructions to look at the cables contained within them and to incorporate them into our work product. Shortly after this, I also noticed the diplomatic cables were being referred to in products from the corps level, U.S. Forces Iraq or USF-I. Based upon Captain Lim's direction to become familiar with its contents, I read virtually every published cable concerning Iraq. I also began scanning database and other -- and reading other random cables that piqued my curiosity.

It was around this time in early to mid-January 2010 that I began searching the database for information on Iceland. I became interested in Iceland due to the IRC conversations I viewed in the WLO channel discussing an issue called "Icesave." At this time, was not very familiar with the topic, but it seemed to be a big issue for those participating in the conversation. This is when I decided to investigate and conduct a few searches on Iceland and find out more.

At the time, did not find anything -- I did not find anything discussing the Icesave issue, either directly or indirectly. I then conducted an open source search for Icesave. I then learned that Iceland was involved in the dispute with the United Kingdom and the Netherlands concerning the financial collapse of one or more of Iceland's banks. According to open source reporting, much of the public controversy involved the United Kingdom's use of anti-terrorism legislation against Iceland in order to freeze Icelandic assets for payments of the guarantees for UK depositors that lost money.

Shortly after returning from mid-tour leave, I returned to the Net-Centric Diplomacy portal to search for information on Iceland and Icesave as the topic had not abated on the WLO IRC channel. To my surprise, on 14 February 2010, I found the cable 10 Reykjavík 13 which referenced the Icesave issue directly. The cable, published on 13 January 2010, was just over two pages in length. I read the cable

and quickly concluded that Iceland was, essentially, being bullied, diplomatically, by two larger European powers. It appeared to me that Iceland was out of viable options and was coming to the U.S. for assistance. Despite their quiet request for assistance, it did not appear that we were going to do anything. From my perspective, it appeared that we were not getting involved due to the lack of long-term geopolitical benefit to do so.

After digesting the contents of 10 Reykjavík 13, I debated on whether this was something I should send to the WLO. At this point, the WLO had not published nor acknowledged receipt of the CIDNE-I and CIDNE-A SIGACTs tables. Despite not knowing if the SIGACTs were a priority for the WLO, I decided the cable was something that would be important and I felt I might be able to right a wrong by having them publish this document.

I burned the document -- or I burned the information onto a CD-RW on 15 February 2010, took it to my CHU, and saved it onto my personal laptop. I navigated to the WLO website via TOR connection, like before, and uploaded the document via the secure form. Amazingly, the WLO published 10 Reykjavík 13 within hours, proving that the form worked and that they must have received the SIGACT tables.

Facts regarding the unauthorized disclosure -- unauthorized storage and disclosure of the 12 July 2007 aerial weapons team or AWT

video. During the mid-tour -- or mid-February time frame, the 2nd Brigade Combat Team, 10th Mountain Division targeting analyst, then Specialist Jihrleah W. Showman and others discussed a video that Ms. Showman had found on the T-drive. The video depicted several individuals being engaged by an aerial weapons team. At first, I did not consider the video very special as I have viewed the countless other war-tore -- war war-porn type videos depicting combat. However, the recording of audio comments by the aerial weapons team and crew and the second engagement in the video of an unarmed bongo truck troubled me.

Ms. Showman and a few other analysts and officers in the T-SCIF commented on the video and debated whether the crew violated the rules of engagement or ROE in the second engagement. I shied away from this debate, instead conducted some research on the event. I wanted to learn about what happened and whether there was any background to the events of the day that the event occurred, 12 July 2007.

Using Google, I searched for the event by its date and general location. I found several news accounts involving two Reuters employees who were killed during the aerial weapon team's engagement. Another story explained that Reuters had requested for a video -- requested for a copy of the video under the Freedom of Information Act or FOIA. Reuters wanted to view the video in order

to be able to understand what had happened and to improve their safety practices in combat zones. A spokesperson for Reuters was quoted saying that the video might help avoid a reoccurrence of the tragedy and believed there was a compelling need for the immediate release of the video.

Despite the submission of the FOIA request, the news account explained that CENTCOM replied to Reuters stating that they could not give a timeframe for considering a FOIA request and that the video may no longer -- might no longer exist. Another story I found, written a year later, said that, even though Reuters was still pursuing their request, they still do not receive a formal response or written determination in accordance with FOIA.

The fact that neither CENTCOM nor Multi-National Forces, Iraq or MNF-I, would not voluntarily release the video troubled me further. It was clear to me that the event happened because the aerial weapons team mistakenly identified the Reuters employees as a potential threat and that the people in the bongo truck were merely attempting to assist the wounded. The people in the van were not a threat, but were merely good Samaritans.

The most alarming aspect of the video, to me, however, was the seemingly delightful bloodlust the aerial weapons -- they appeared to have. They dehumanized the individuals they were engaging and seemed to not value human life by referring to them as

"dead bastards" and congratulating each other on the ability to kill in large numbers. At one point in the video, there's an individual on the ground attempting to crawl to safety; the individual is seriously wounded. Instead of calling for medical attention to the location, one of the aerial weapons team crew members verbally asks for the wounded person to pick up a weapon so that he can have a reason to engage. For me, this seems similar to a child torturing ants with a magnifying glass.

While saddened by the aerial weapons teams crew -- or the aerial weapon teams crew's lack of concern about human life, I was disturbed by the response the discovery of injured children at the scene. In the video, you can see that the bongo truck driving up to assist the wounded individual. In response, the aerial weapons team crew assumes the individuals are a threat. They repeatedly request for authorization to fire on the bongo truck and, once granted -- and once granted, they engage the vehicle at least six times.

Shortly after the second engagement, a mechanized infantry unit arrives at the scene. Within minutes, the aerial weapons team crew learns that the children -- that children were in the van and, despite the injuries, the crew exhibits no remorse. Instead, they downplay the significance of their actions saying, "Well, it's their fault for bringing their kids into a battle." The aerial weapons team crew members sound like they lack sympathy for the children or

the parents. Later, in a particularly disturbing manner, the aerial weapons team crew verbalizes enjoyment at the sight of one of the ground vehicles driving over a body -- or one of the bodies.

As I continued my research, I found an article discussing a book, *The Good Soldiers*, written by *Washington Post* writer David Finkel. In Mr. Finkel's book, he writes about the aerial weapons team attack. As I read an online excerpt on Google Books, I followed Mr. Finkel's account of the event along with the video. I quickly realized that Mr. Finkel was quoting, I feel, in verbatim, the audio communications of the aerial weapons team crew. It is clear to me that Mr. Finkel obtained access and a copy of the video during his tenure as an embedded journalist.

I was aghast at Mr. Finkel's portrayal of the incident. Reading his account, one would believe the engagement was somehow justified as payback for an earlier attack that led to the death of a Soldier.

Mr. Finkel -- Mr. Finkel ends his account of the engagement by discussing how a Soldier finds an individual still alive from the attack. He writes that the Soldier finds him and sees him gesture with his two forefingers together, a common method in the Middle East to communicate that they are friendly. However, instead of assisting him, the Soldier makes an obscene gesture extending his middle finger. The individual apparently dies shortly thereafter. Reading

this, I can only think of how this person was simply trying to help others and then quickly finds he needs help as well. To make matters worse, in the last moments of his life, he continues to express his friendly -- this -- his friendly intent, only to find himself receiving this well-known gesture of unfriendliness. For me, it's all a big mess and I'm left wondering what these things mean and how it all fits together and it burdens me emotionally.

I saved a copy of the video on my workstation. I searched for and found the rules of engagement, the rules of engagement annexes, and a flow chart from the 2007 time period as well as an unclassified rules of engagement smart card from 2006.

On 15 February 2010, I burned these documents onto a CD-RW the same time I burned the 10 Reykjavík 13 cable onto a CD-RW. At the time, I placed the video and rules of engagement information onto my personal laptop in my CHU. I planned to keep this information there until I redeployed in summer of 2010. I planned on providing this to the Reuters office in London to assist them in preventing events such as this in the future. However, after the WLO published 10 Reykjavík 13, I altered my plans. I decided to provide the video and rules of engagement to them so that the -- so that Reuters would have this information before I redeployed from Iraq.

On about 21 February 2010, as described above, I used the WLO submission form and uploaded the documents. The WLO released the

video on 5 April 2010. After the release, I was concerned about the impact of the video and how it would be perceived by the general public. I hoped that the video would be -- I hoped that the public would be as alarmed as me about the conduct of the aerial weapons team members. I wanted the American public to know that not everyone in Iraq and Afghanistan were targets that needed to be neutralized, but rather people who were struggling to live in the pressure cooker environment of what we call asymmetric warfare.

After the release, I was encouraged by the response in the media and general public who observed the aerial weapons team video. As I hoped, others were just as troubled, if not more troubled than me, by what they saw.

At this time, I began seeing reports claiming that the Department of Defense and CENTCOM could not conform -- cannot confirm the authenticity of the video. Additionally, one of my supervisors, Captain Casey Fulton, stated her belief that the video was not authentic. In her response, I decided to ensure that the authenticity of the video would not be questioned in the future.

On 25 February 2010, I emailed Captain Fulton a link to the video that was on our T-drive and a copy of the video published by WLO that was collected by the open source Center so she could compare them herself.

Around this time frame, I burned a second CD-RW containing the aerial weapons team video. In order to make it appear authentic, I placed a classification sticker and wrote "Reuters FOIA REQ" on its face. I placed the CD-RW in one of my personal CD cases containing a set of "Starting Out in Arabic" CDs. I planned on mailing the CD-RW to Reuters after I redeployed so that they could have a copy that was unquestionably authentic.

Almost immediately after submitting the aerial weapons team video and the rules of engagement documents, I notified the individuals in the WLO IRC to expect an important submission. I received a response from an individual going by the handle of "Office." At first, our conversations were general in nature but over time, as our conversations progressed, I assessed this individual to be an important part of the WLO.

Due to the strict adherence of anonymity by the WLO, we never exchanged identifying information. However, I believe the individual was likely Mr. Julian Assange, Mr. Daniel Schmidt, or a proxy representative of Mr. Assange and Schmidt.

As the communications transferred from IRC to the Jabber client, I gave "Office" and later "Press Association" the name of Nathaniel Frank in my address book, after the author of -- after the author of a book I read in 2009. After a period of time, I developed what I felt was a friendly relationship with Nathaniel. Our mutual

interest in information technology and politics made our conversations enjoyable. We engaged in conversation often, sometimes as long as an hour or more. I often looked forward to my conversations with Nathaniel after work.

The anonymity that was provided by TOR, the Jabber client, and the WLO's policy allowed me to feel I could just be myself, free of the concerns of social labeling and perceptions that are often placed upon me in real life. In real life, I lacked a close friendship with the people I worked with in my section, the S-2 section, the S-2 sections in subordinate battalions, and the 2nd Brigade Combat Team as a whole. For instance, I lacked close ties to my roommate due to his discomfort regarding my perceived sexual orientation.

Over the next few months, I stayed in frequent contact with Nathaniel. We conversed on nearly a daily basis and I felt that we were developing a friendship. The conversations covered many topics and I enjoyed the ability to talk about pretty much anything and not just the publications that the WLO was working on.

In retrospect, I realize that these dynamics were artificial and were valued more by myself than Nathaniel. For me, these conversations represented an opportunity to escape from the immense pressures and anxiety that I experienced and built up throughout the deployment. It seems that as I tried harder to fit in

at work, the more I seemed to alienate my peers and lose respect, trust, and the support I needed.

Facts regarding the unauthorized disclosure -- or unauthorized storage and disclosure of documents related to the detainments by the Iraqi Federal Police or FP and the Detainee Assessment Briefs, and the USACIC -- United States Army Counterintelligence Center report. On 27 February 2010, a report was received -- a report was received from a subordinate battalion. The report described an event in which the Federal Police detained, or FP, detained 15 individuals for printing anti-Iraqi literature.

By 2 March 2010, I received instructions from an S-3 section officer in the 2nd Brigade Combat Team, 10th Mountain Division Tactical Operations Center or TOC to investigate the matter and figure out who these "bad guys" were and how significant this event was for the Federal Police.

Over the course of my research, I found that none of the individuals had previous ties to anti-Iraqi actions or suspected terrorist militia groups. A few hours later, I received several photos from the scene from the subordinate battalion. They were accidentally sent to an officer on a different team than the S-2 section and she forwarded them to me. These photos included pictures of the individuals, pallets of unprinted paper, and seized copies of the final printed material -- or printed document and a high-

resolution photo of the printed material itself. I printed a blown up copy of the high-resolution photo, I laminated it for ease of use and transfer, I then walked to the TOC, and delivered the laminated copy to our category two interpreter. She reviewed the information and, about a half an hour later, delivered a rough, written transcript in English to the S-2 section. I read the transcript and followed up with her asking her for her take on the contents. She said it was easy for her to transcribe verbatim since I blew up the photograph and laminated it. She said the general nature of the document was benign.

The documentation, as I assessed as well, was merely a scholarly critique of the, then, current Iraqi prime minister, Nouri al-Maliki. It detailed corruption with the cabinet of al-Maliki's government and the financial impact of his corruption on the Iraqi people.

After discovering this discrepancy between the Federal Police's report and the interpreter's transcript, I forwarded this discovery to the TOC OIC and the Battle NCOIC. The TOC OIC and the overhearing Battle Captain informed me that they didn't want -- or that they didn't need or want to know this information any more. They told me to "drop it" and to just assist them and the Federal Police in finding out where more of these print shops creating "anti-Iraqi literature" might be. I couldn't believe what I heard -- or I

couldn't believe what I heard and I returned to the T-SCIF and complained to the other analysts and my section NCOIC about what happened. Some were sympathetic, but none wanted to do anything about it. I'm the type of person who likes to know how things work, and, as an analyst, this means I always want to figure out the truth. Unlike other analysts in my section or other sections within the 2nd Brigade Combat Team, I was not satisfied with just scratching the surface of producing canned or cookie-cutter assessments. I wanted to know why something was the way it was and what we could do to correct or mitigate a situation.

I knew that if I continue to assist the Baghdad Federal Police in identifying the political opponents of Prime Minister al-Maliki, those people would be arrested and in the custody of the Special Unit of the Baghdad Federal Police, very likely tortured and not seen again for a very long time, if ever.

Instead of assisting the Special Unit of the Baghdad Federal Police, I had decided to take the information and disclose it to the WLO in the hope that, before the upcoming 7 March 2010 election, they could generate some immediate press on the issue and prevent this unit of the Federal Police from continuing to crack down on political opponents of al-Maliki.

On 4 March 2010, I burned the report, the photos, the high-resolution copy of the pamphlet, and the interpreter's hand-written

transcript onto a CD-RW. I took the CD-RW to my CHU and copied the data onto my personal computer. Unlike the times before, instead of uploading the information through the WLO website's submission form, I made a Secure File Transfer Protocol or SFTP connection to a Cloud drop box operated by the WLO. The drop box contained a folder that allowed me to upload directly into it. Saving files into this directory allowed me -- allowed anyone with log in access to the server to view and download them. After downloading these file -- or after uploading these files to the WLO on 5 March 2010, I notified Nathaniel over Jabber.

Although sympathetic, he said that the WLO needed more information to confirm the event in order for it to be published or to gain interest in the international media. I attempted to provide these specifics, but, to my disappointment, the WLO website chose not to publish this information. At the same time, I began sifting through information from the U.S. SOUTHCOM -- or U.S. Southern Command or SOUTHCOM and Joint Task Force Guantánamo, Cuba or JTF-GTMO. The thought occurred to me, although unlikely -- that I wouldn't be surprised if the -- although unlikely -- that I wouldn't be surprised if the individuals detained by the Federal Police might be turned over back into U.S. custody and ending up in the custody of Joint Task Force Guantánamo.

As I digested -- as I digested through the information on Joint Task Force Guantánamo, I quickly found the Detainee Assessment Briefs or DABs. I previously came across these documents before in 2009 but did not think much of them. However, this time, I was more curious during this search and I found them again.

The DABs were written in standard DoD memorandum format and addressed the Commander, U.S. SOUTHCOM. Each memorandum gave basic and background information about a specific detainee held, at some point, by Joint Task Force Guantánamo. I have always been interested on the issue of the moral efficacy of our actions surrounding Joint Task Force Guantánamo. On the one hand, I've always understood the need to detain and interrogate individuals who might wish to harm the United States and our allies, however, I felt that there -- that that was -- however, I felt that's what we were doing -- what we were trying to do at Joint Task Force Guantánamo. However, the more I became educated on the topic, it seemed that we found ourselves holding an increasing number of individuals indefinitely that we believed, or knew, to be innocent, low-level foot support -- low-level foot soldiers that we didn't -- that did not have useful intelligence and would be released if they were still in theater -- if they were still held in theater.

I also recall that, in early 2009, the then newly elected president, Barack Obama, stated that he would close Joint Task Force

Guantánamo and that the facility compromised our standing in the world and diminished our "moral authority." After familiarizing myself with the Detainee Assessment Briefs, I agreed. Reading through the Detainee Assessment Briefs, I noticed that they were not analytical products. Instead, they contained summaries of tear-line versions of interim intelligence reports that were old or unclassified. None of the DABs contained names of sources or quotes from a Tactical Interrogation Reports or TIRs. Since the DABs were being sent to the U.S. SOUTHCOM Commander, I assessed that they were intended to provide very general background information on each detainee and not a detailed assessment.

In addition to the manner in which DABs were written, I recognized that they were at least several years old and discussed detainees that were already released from Joint Task Force Guantánamo. Based on this, I determined that the DABs were not very important from either an intelligence or national security standpoint.

On 7 March 2010, during my Jabber conversations with Nathaniel, I asked him if he thought the DABs were of any use to anyone. Nathaniel indicated, although he didn't -- did not believe that they were of political significance, he did not believe -- he did believe that they could be used to merge into the general, historical account of what occurred at Joint Task Force Guantánamo.

He also thought that the DABs might be helpful to a legal counsel of those currently and previously held at JTF-GTMO.

After this discussion, I decided to download the DABs. I used an application called Wget to download the DABs. I downloaded Wget off of the NIPRNET laptop in the T-SCIF like other programs. I saved that onto a CD-RW and placed the executable in my My Documents directory of my user profile on the DCGS-A SIPRNET workstation.

On 7 March 2010, I took the list of four link -- I took the list of links for the Detainee Assessment Briefs and Wget downloaded them sequentially. I burned the DABs onto a CD-RW and took it into my CHU and copied them to my personal computer.

On 8 March 2010, I combined the Detainee Assessment Briefs with the United States Army Counterintelligence Center Report on the -- on the WLO into a compressed zip file. Zip files contain multiple files which are compressed to reduce their size. After creating the zip file, I uploaded the file onto their Cloud drop box via Secure File Transfer Protocol. Once these were uploaded, I notified Nathaniel that the information was in the X directory which had been designated for my use.

Earlier that day, I downloaded the USACIC report on WLO. As discussed above, I previously reviewed the report on numerous occasions and, although I saved the document onto the workstation before, I could not locate it. After I found the document again, I

downloaded it to my workstation and saved it onto the same CD-RW as the Detainee Assessment Briefs described above.

Although my access included a great deal of information, I decided I had nothing else to send the WLO after sending the Detainee Assessment Briefs and the USACIC report. Up to this point, I had sent them the following: the CIDNE-I and CIDNE-A SIGACT tables; the Reykjavík 13 Department of State cable; the 12 July 2007 aerial weapons team video and the 2006-2007 rules of engagement documents; the SIGACT report and supporting documents concerning the 15 individuals detained by the Baghdad Federal Police; the U.S. SOUTHCOM and Joint Task Force Guantánamo Detainee Assessment Briefs; the USACIC report on the WikiLeaks website -- on the WikiLeaks organization and website.

Over the next -- over the next few weeks, I did not find -- or I did not send any additional information to the WLO. I considered -- I continued to converse with Nathaniel over the Jabber client and in the WLO IRC channel. Although I stopped sending documents to WLO, no one associated with the WLO pressured me into giving more information. The decisions that I made to send documents and information to the WLO and website were my own decisions and I take full responsibility for my actions.

Facts regarding the unauthorized storage and disclosure of other government documents. On 22 March 2010, I downloaded two

documents. I found these documents over the course of my normal duties as an analyst. Based on my training and the guidance of my superiors, I looked at as much information as possible. Doing so provided me with the ability to make connections others might miss. On several occasions during the month of March, I accessed information from a government entity. I read several documents from a section within this government entity. The content of two of these documents upset me greatly. I have difficulty believing what this section was doing.

On 22 March 2010, I downloaded the two documents that I found troubling, I compressed them into a zip file named "blah.zip" and burned them onto a CD-RW. I took the CD-RW to my CHU and saved the file to my personal computer. I uploaded the information to the WLO website using the designated drop box.

Facts regarding the unauthorized storage and disclosure of the Net-Centric Diplomacy Department Of State cables. In late March of 2010, I received a warning over Jabber from Nathaniel that the WLO website would be publishing the aerial weapons team video. He indicated that the WLO would very likely -- would be very busy and the frequency and intensity of our Jabber conversations decreased significantly.

During this time, I had nothing but work to distract me. I read more of the diplomatic cables published on the Department of

State Net-Centric Diplomacy server. With my insatiable curiosity and interest in geopolitics, I became fascinated with them. I read not only the cables on Iraq, but also about countries and events I found interesting. The more I read, the more I was fascinated by the way we dealt with other nations and organizations. I also began to think that they documented backdoor deals and seemingly criminal activity that didn't seem characteristic of the de facto leader of the free world.

Up to this point, during deployment, I had issues that I struggled with and difficulty at work. Of the documents released, the cables were the only ones I was not absolutely certain wouldn't -- couldn't harm the United States. I conducted research on the cables published on the net -- on Net-Centric Diplomacy, as well as how Department of State cables work in general. In particular, I wanted to know how each cable was published on SIPRNET via the Net-Centric Diplomacy.

As part of my open-source research, I found a document published by the Department of State on its official website. The document provided guidance on caption markings for individual cables and handling instructions for their distribution. I quickly learned that the caption markings clearly detailed the sensitivity level of a Department of State cable. For example, "NODIS," or "No Distribution," was used for messages of the highest sensitivity and

were only distributed to the authorized recipients. The SIPDIS or SIPRNET Distribution caption was applied only to reporting at other information messages that were deemed appropriate for a release of a wide number -- to a wide number of individuals.

According to the Department of State guidance for a cable to have the SIPDIS -- that caption, it could not include other captions that were intended to limit distribution. The SIPDIS caption was only for information that could be shared with anyone with access to SIPRNET. I was aware that thousands of military personnel, DoD, Department of State, and other civilian agencies have easy access to the cables and the fact that the SIPDIS caption was only for wide distribution made sense to me, given that the vast majority of the Net-Centric Diplomacy cables were not classified. The more I read the cables, the more I came to the conclusions that this was the type of information that should be -- that this type of information should become public. I once read and used a quote on open diplomacy written after the First World War and how the world would be a better place if states would avoid making secret pacts and deals with and against each other.

I thought these cables were a prime example of a need for a more open diplomacy. Given all the Department of State information I read, the fact that most of the cables were unclassified and that all the cables had the SIPDIS caption, I believed that the public release

of these cables would not damage the United States. However, I did believe the cables might be embarrassing, since they represented very honest opinions and assessments behind or statements behind the backs of other nations and organizations.

In many ways, these cables are a catalog of cliques and gossip. I believe exposing this information might make some within the Department of State and other government entities unhappy. On 22 March 2010, I began downloading a copy of the SIPDIS cables using the program Wget described above. I used instances of the Wget application to download the Net-Centric Diplomacy cables in the background. As I worked on my daily tasks, the Net-Centric Diplomacy cables were downloaded from 28 March 2010 to 9 April 2010. After downloading the cables, I saved them onto a CD-RW. These cables went from the earliest dates in Net-Centric Diplomacy to 28 February 2010. I took the CD-RW to my CHU on 10 April 2010. I sorted the cables on my personal computer, compressed them using the bzip2 compression algorithm described above and uploaded them to the WLO via the designated drop box described above.

On 3 May 2010, I used Wget to download an update of the cables for the months of 20 -- for the months of March 2010 and April 2010 and saved the information onto a zip file and burn it to a CD-RW. I took -- I then took the information--I then took the CD-RW to my CHU and saved them to my computer. I later found that the file

was corrupted during the transfer. Although I intended to re-save another copy of these cables, I was removed from the T-SCIF on 8 May 2010 after an altercation.

Facts regarding the unauthorized storage and disclosure of the Garani Farah Province, Afghanistan 15-6 investigation and videos. In late March 2010, I discovered a U.S. CENTCOM directory only 2009 airstrike in Afghanistan. I was searching CENTCOM for information I could use as an analyst. As described above, this was something that myself and other analysts and officers did on a frequent basis. As I reviewed the documents, I recalled the incident and what happened. The airstrike occurred in the Garani Village of the Farah Province in northwestern Afghanistan. They receive worldwide press and -- worldwide press coverage during the time as it was reported that up to 100 to 150 Afghan civilians, mostly women and children, were accidentally killed during the airstrike.

After going through the report and its annexes, I began to review the incident as being similar to the 12 July 2007 aerial weapons team engagements in Iraq. However, this event was noticeably different in that it involved a significantly higher number of individuals, larger aircraft, and much heavier munitions. Also, the conclusion of the report are even more disturbing than those of the 12 July 2007 incident. I did not see anything in the 15-6 report or its annexes that give away sensitive information. Rather, the

investigation and its conclusions help explain how this incident occurred and what those involved should have done and how to avoid an event like this from occurring again.

After investigating the report and its annexes, I downloaded the 15-6 investigation, PowerPoint presentations, and several other supporting documents to my DCGS-A workstation. I also downloaded three zip files containing the videos of the incident. I burned this information onto a CD-RW and transferred it to the personal computer in my CHU. Either later that day or the next day I uploaded the information to the WLO website, this time using a new version of the WLO website submission form. Unlike other times using the submission form above, I did not activate the TOR annonymizer.

Your Honor, this concludes my statement and facts for this providence inquiry.

MJ: All right. Looking at the time, my proposal for the way forward would be to take the recess that we were discussing earlier, go over the charged documents briefly, and then recess for lunch and then begin the rest of the providence inquiry. Is that acceptable to both sides or would you prefer something different?

CDC[MR.COOMBS]: That's fine with the defense, Your Honor.

TC[MAJ FEIN]: Yes, ma'am, the United States asks for 10 minutes for that recess.

MJ: All right. Court is in recess until 25 minutes after 12.

**[The Article 39(a) session recessed at 1217, 28 February 2013.]**

**[The Article 39(a) session was called to order at 1231, 28 February 2013.]**

MJ: This Article 39(a) session is called to order. Let the record reflect that all parties present when the court last recessed are again present in court.

Now, Major Fein, I understand there has been an additional appellate exhibit marked. Would you like to describe it for the record?

TC[MAJ FEIN]: Yes, ma'am, Appellate Exhibit -- what has been marked as Appellate Exhibit 501 is a compilation -- two different binders combined all the different charged documents for which Private First Class Manning is pleading guilty today to. And, also, for the record, Private First Class Manning is currently located at the panel box in the back row with a copy of Appellate Exhibit 501 and a charge sheet in front of him. Another copy of the Appellate Exhibit 501 -- the record copy is excuse me, the record copy is in front of Private First Class Manning and the Court has a copy in front of her as well.

MJ: All right. Thank you. All right, PFC Manning, what I'd like to do is go through -- there are two binders; do you have a copy of them in front of you?

ACC: Yes, Your Honor.

MJ: All right. I like to go through Appellate Exhibit 501 and have you looked through the binder with me when we go through this to make sure that you either identify or don't -- whether these documents are the actual charged documents that your pleading guilty to.

Let's look at tab one ----

ACC: Yes, Your Honor.

MJ: ---- which would be the charged documents for Charge II, Specification 2, which would be a video file named "12 July 07 CZ Engagement Zone 30 GC Anyone.avi". Now, you're looking at a video. Have you had an opportunity to look at this video?

ACC: Yes, Your Honor.

MJ: And is it the video that has been charged in the -- in Specification 2 of Charge II?

ACC: Yes, Your Honor.

MJ: All right. Now, unlike the rest of the charges, this one says, "a video file." So, is it classified or not classified?

ACC: It is not, Your Honor.

MJ: All right. Thank you. Let's look at tab two. Please take a look at the documents through tab two and let me know when you're finished.

**[The accused did as directed.]**

ACC: I'm finished, Your Honor.

MJ: Are the pages on tab -- enclosed in tab two the charged documents in Specification 3 of Charge II which would be more than one classified memorandum produced by a United States Government agency?

ACC: Yes, Your Honor.

MJ: All right. And are they, in fact, classified?

ACC: They are, Your Honor, yes.

MJ: Let's look at tab three. Once again, same procedure for all these tabs, just take a look through them and let me know when you're finished.

**[The accused did as directed.]**

ACC: I'm finished, Your Honor.

MJ: All right. Are the pages at tab three the charged documents in Specification 15 which would be a classified record produced by a United States Army intelligence organization?

ACC: Yes, Your Honor.

MJ: Okay. And are they, in fact, classified as well?

ACC: Yes, Your Honor.

TC[MAJ FEIN]: Your Honor, I'm sorry to interrupt, but is it possible that Private First Class Manning put the binder in his lap just while he's flipping the pages?

MJ: All right. I think the goal is -- yeah, just keep it down. Thank you PFC Manning. I know this is making it a little bit more difficult. Let's look at tab four.

ACC: Yes, Your Honor.

MJ: All right. Are you finished with the documents in tab four?

ACC: I am, Your Honor.

MJ: Are those the charge documents for Specification 5 of Charge II which would be more than 20 classified records from the Combined Information Data Network Exchange-Iraq database?

ACC: They are, Your Honor.

MJ: And are they classified as well?

ACC: Yes.

MJ: All right. Let's look at tab five.

ACC: Yes, Your Honor.

MJ: All right. Are these documents at tab five the charged documents for Specification 7 of Charge II that would be more than 20 classified records from the Combined Information Data Network Exchange-Afghanistan database?

ACC: They are, Your Honor.

MJ: All right. And there they classified as well?

ACC: Yes, Your Honor.

MJ: Let's look at tab six.

ACC: Yes, Your Honor.

MJ: All right. Are the documents at tab six the charged documents for Specification 9 of Charge II, that is, more than three classified records from the United States Southern Command database?

ACC: It is, Your Honor.

MJ: Are they classified as well?

ACC: Yes, Your Honor, they are.

MJ: All right. Let's look at tab seven.

ACC: I'm finished, Your Honor.

MJ: Are the documents at enclosure seven the charged documents in Specification 10 of Charge II that would be more than five classified records relating to the military operation in Farah Province, Afghanistan occurring on or about 4 May 2009?

ACC: They are, Your Honor.

MJ: And are they classified as well?

ACC: Most of it is, Your Honor.

MJ: Let's look at tab eight.

ACC: Yes, Your Honor.

MJ: Is this the document that is charged in Specification 14 of Charge II which would be a classified Department of State cable entitled Reykjavík 13?

ACC: It is, Your Honor.

MJ: Is a classified?

ACC: Yes, ma'am.

MJ: All right. Let's look at enclosure nine.

ACC: I am finished, Your Honor.

MJ: All right. Are the documents at tab nine the charged documents in Specification 13 of Charge II which would be more than 75 classified United States Department of State cables?

ACC: Yes, ma'am.

MJ: Are they class -- you testified earlier that most of the Department of State cables were not classified. Are these documents in enclosure nine classified?

ACC: These ones, yes, Your Honor.

MJ: And are you convinced there's over 70 -- more than 75 of them?

ACC: Yes, Your Honor, definitely.

MJ: Does either side desire any further inquiry with respect to Appellate Exhibit 501?

TC[MAJ FEIN]: No, Your Honor.

CDC[MR.COOMBS]: No, Your Honor.

MJ: All right. This appears to be a good time to break for lunch. How long would the parties like?

CDC[MR.COOMBS]: 1400.

MJ: Does that work for the government?

TC[MAJ FEIN]: Yes, ma'am.

MJ: All right. Court is in recess until 1400.

**[The Article 39(a) session recessed at 1244, 28 February 2013.]**

**[The Article 39(a) session was called to order at 1408, 28 February 2013.]**

MJ: This Article 39(a) session is called to order. Let the record reflect all parties present when the court last recessed are again present in court.

TC[MAJ FEIN]: Ma'am, for the record, Private First Class Manning is back at counsel's table.

MJ: All right. Okay, PFC Manning, let's continue on, then, with your providence inquiry.

ACC: Yes, ma'am.

MJ: All right. I'm going to explain the elements of the offenses for which you've pled guilty.

By "elements," I mean those facts which the prosecution would have to prove beyond a reasonable doubt before you could be found guilty if you have pled not guilty. When I state each element, ask yourself two things: first, is the element true and, second, whether you want to admit that it's true. After I list the elements for you, be prepared to talk to me about the facts regarding the offenses.

I want you to take a look at Specifications 2, 3, 5, 7, 9, 10, and 15 of Charge II as you pled them. These specifications

allege the offense of -- as originally charged, alleged the offense of transmitting defense information in violation of Title 18, United States Code section 793(e) and Article 134, UCMJ. Your counsel has entered a plea of guilty by exceptions and substitutions for you to the lesser included offense of conduct prejudicial to good order and discipline and service discrediting conduct under Article 134, clauses one and two. By pleading guilty to this offense, you're admitting that the following elements are true and accurately describe what you did:

Element one: that, at or near Contingency Operating Station Hammer, Iraq;

Specification two: between on or about 14 February 2010 and 21 February 2010, you, without authorization, had possession of, access to, or control over a video named "12 July 07 CZ Engagement Zone 30 GC Anyone.avi".

Specification 3: between on or about 17 March and 22 March 2010, you, without authorization, had possession of, access to, or control over more than one classified memorandum produced by a United States Government agency.

Specification 5: between on or about 5 January 2010 and 3 February 2010, you, without authorization, had possession of, access to, or control over more than 20 classified records from the Combined Information Data Network Exchange-Iraq database.